Whistler Design Preview
April 20 & 21

Group Policy - RSoP

Michael Dennis
Program Manager
IntelliMirror – Group Policy
Microsoft Corporation

Session Goals

- Brief review of:
  - Current limitations
  - Plans for Whistler
- Issues driving RSoP Requirements
- Current Windows 2000 Tools
- Share RSoP development information
  - History, status, plans

Session Goals

You should leave understanding:

- Customer needs addressed by RSoP
- Whistler changes that support RSoP tools
- Description of the tool we will ship
  - What it will do
  - What it won't do

Current Group Policy Infrastructure Limitations

- No public methods of determining what each extension to Group Policy will do or has done with a given list of GPOs – Therefore:
  - No RSoP tool from MS
  - No consistent method for ISV's to build an RSoP tool
- To view a GPO requires write access
- General Active Directory auditing not Group Policy focused
- No reporting capabilities

RSoP

We have an enhanced infrastructure

- Using WMI
- Public method of exposing what each extension would do or has done
- Isolates user of tool from the GPO store
  - Allows reading of data without write access
- Enables the creation of rich products and tools for diagnostic and planning purposes

Why Resultant Set of Policy (RSoP)???????

What customers have to do today without full featured products to do RSoP

- Review of Group Policy processes required in Windows 2000:
  - Intense documenting
  - Testing after setup in a test lab required
  - Troubleshooting challenges
  - Monitoring challenges

- Question coming – Are these the things you do today? What else?

Documenting Group Policy

What customers need to do today

Keeping Track of Special Settings May Allow You to Resolve Conflicts at a Glance

Name	Container	Policy	Setting	Special
Default	Corporate OU	Change wallpaper		Blue
No Override				
Sales	Sales OU	Change wallpaper		Red
None				
US	Sales-US OU	Change wallpaper		Green
None				

A Database Allows You to Easily Look at All Policies Affecting a Given SDOU

Testing GPOs

Method of determining RSoP today

Suggested Testing Procedure

- Create test accounts and a test security group
- Determine the existing configuration
- Create the GPO and apply it to the test security g
- Log on as a tester and verify effects of the GPO
- Apply the GPO to actual users

Resolving Group Policy Conflicts

- Start the search at the top of the Active Directory tree
- Check the order of precedence
- Check for user or computer conflicts
- Check for No Override or Block Policy Inheritance settings
- Check for Group Policy filtering

Monitoring Group Policy

- Use the Event Log
- Has error condition entries
- Verbose flag allows for detailed information on a per machine/per user basis (non-error cases also)
  - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics RunDiagnosticLoggingGroupPolicy REG_DWORD 1
- Group Policy processing log
  - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
    - GPEditDebugLevel REG_DWORD 0x30002
    - Generates log in %SystemRoot%\Debug\userenv.log

Best Practices

- Limit how often Group Policy is updated (to reduce replication)
- Limit the number of admins who can edit GPOs (to reduce possibility of simultaneous editing)
- Limit inheritance modification, filtering, and loopback (to simplify troubleshooting)
- Limit the number of GPOs that apply to an SDOU (to improve logon performance)
- Test! (to reduce Help desk calls)

Currently available tools

- Group Policy Results tools
  - GPResult.exe – Resource Kit
  - FAZAM 2000 – Full Armor
    - http://www.FullArmor.com
    - Lou Klubenspies (LKlubenspies@FullArmor.com)
- Others in the Resource Kit
  - Group Policy Reference
    - Documents each Administrative Template based policy setting and 111 security policy settings
    - Whistler - Info will be in Help
  - GPOTool.exe

FAZAM 2000 – Full Armor

http://www.FullArmor.com

Group Policy Results

- Gpresult.exe command-line tool displays *general* info on
  - OS Type, Build, and Terminal Services status
  - User name, AD location, domain name/type, profile type/location, security group membership
  - Computer name, AD location, domain name/type, site

Group Policy Results

- Gpresult.exe command-line tool displays *detailed* info on
  - Last time policy applied for user and computer
  - Detailed list of applied GPOs and included extensions
  - Detailed list of registry settings applied (with preferences warning)
  - Detailed list of redirected folders, published and assigned apps, scripts and IPSec settings

Group Policy Results

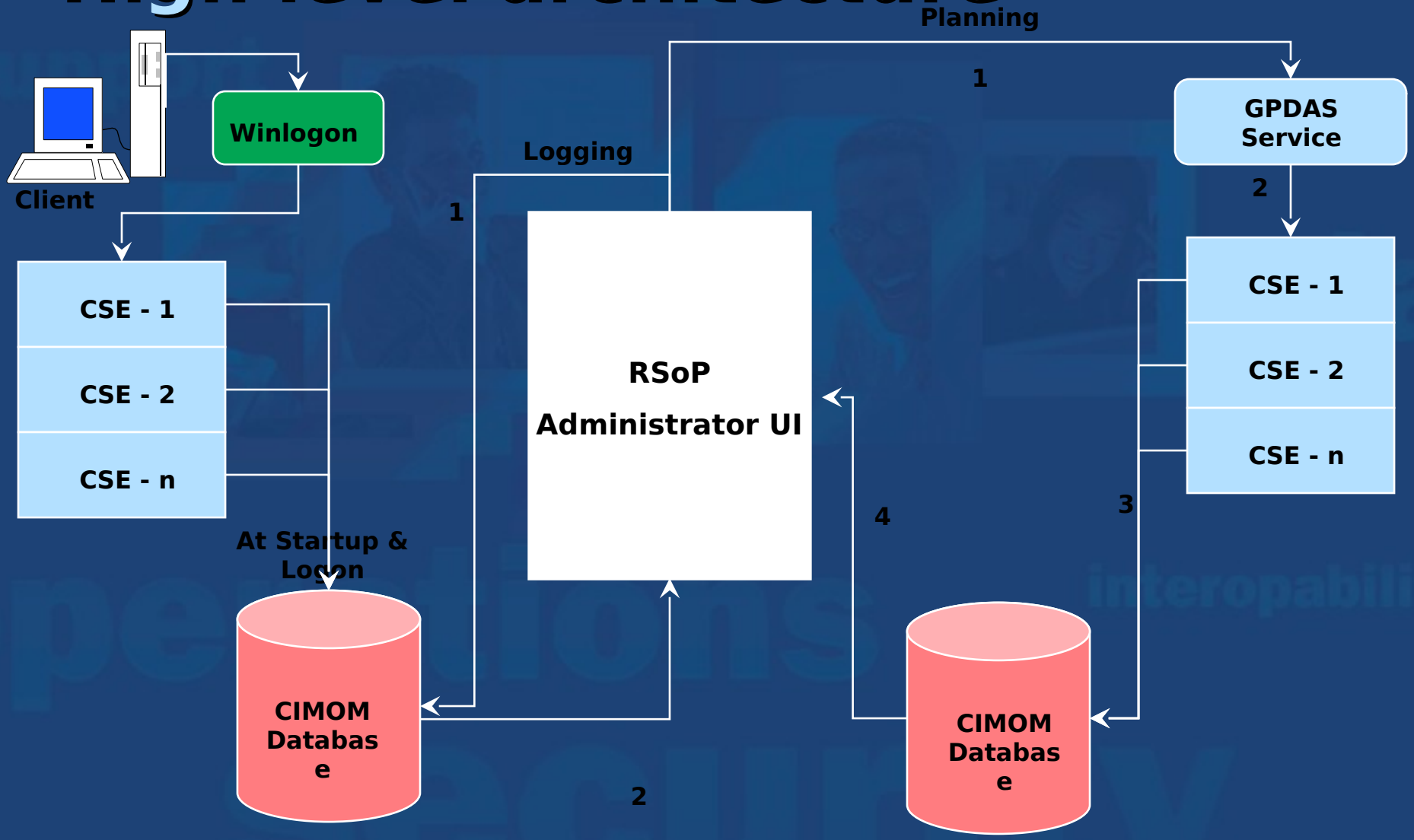
- Gpresult.exe command-line tool displays *no* info on
  - Security policies (use SCE)
  - Internet Explorer Maintenance policies
  - EFS Recovery policies
- Ships with Windows 2000 Resource Kit

RSoP - The Plan
Isolation layer using WMI

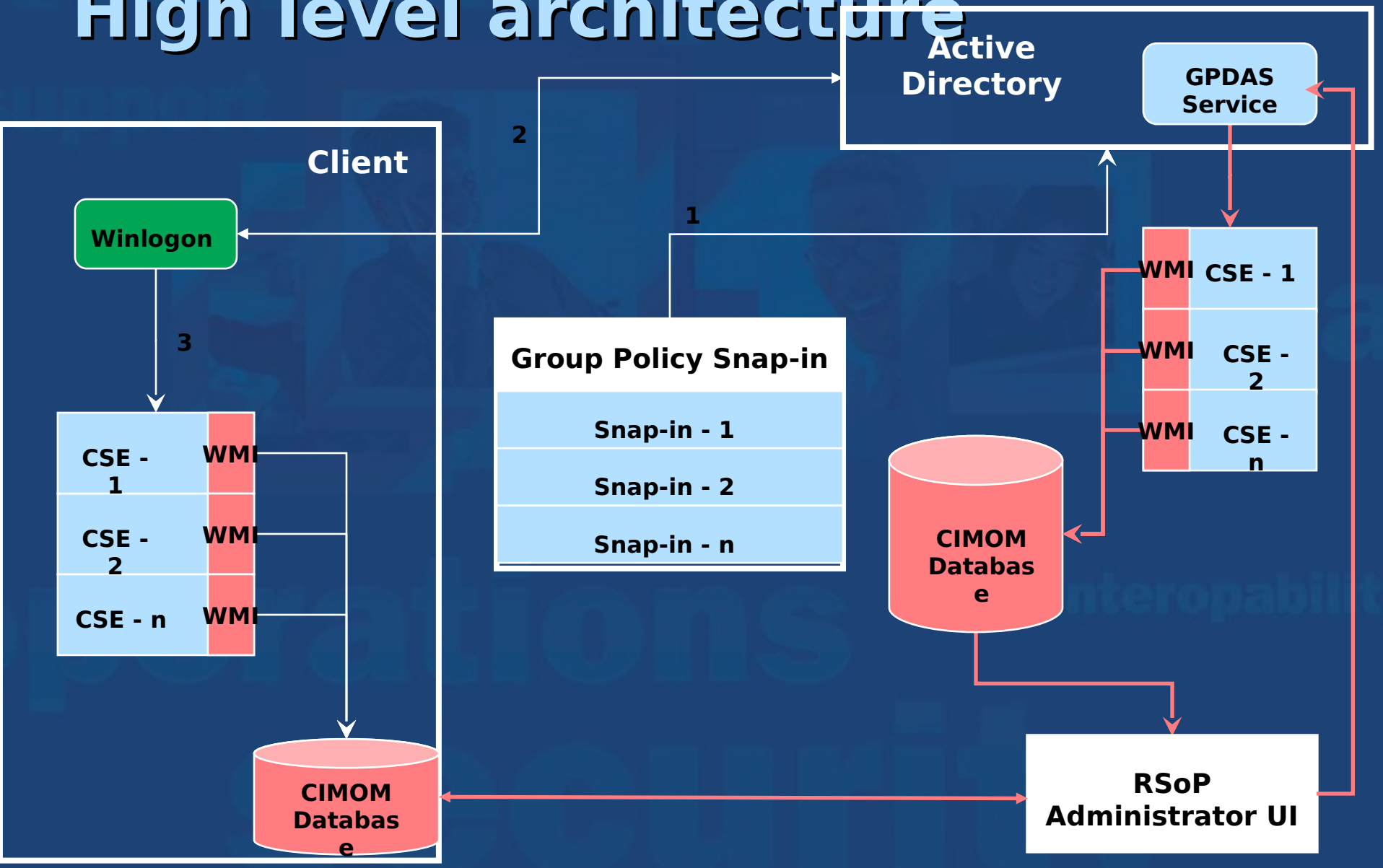
- All current Group Policy client-side extensions have been modified to include a WMI provider
- Publicly expose the schema
- Encourage ISV development based on the new infrastructure

RSoP

High level architecture



Group Policy
High level architecture



RSoP - The Plan

Microsoft will build a base level tool

- Logging mode
  - What was applied?
  - RSoP for a given target
- Planning mode
  - What will be applied?
  - View potential state based on:
    - User, Computer
    - Site, Domain, OU
    - Security Group membership
- For each policy indicate source GPO
- Precedence order of settings
- Settings failed to apply indication
- Similar look and feel to the Group Policy snap-in

ISV Opportunities
Tools based on WMI

- Compare/Alert on differences between planned vs. actual RSoP
- Compare/Alert on differences between saved instance and current view
- Reports (print, web, etc)
- Change management
- Integration with existing management tools

ISV Opportunities
Not just for RSoP tools

- Needs in other areas can be mitigated by having an RSoP infrastructure and products available that exploit it fully
  - No GP specific Auditing capabilities
    - Tool could be build to monitor specific GPOs or target OU (RSoP) and alert on any changes from a saved result
  - No READ only access to a GPO through the Group Policy UI
    - RSoP infrastructure is read only and exposes all settings
    - Tool could be built to provide read

Questions?


WHERE DO YOU WANT TO
go
TODAY?
Microsoft